

第6章 人工呼吸器に見るセーフティ・クリティカル・システム設計

柳川誠介

2重3重のバックアップで生命を守る

ここでは，生命維持装置の一つである人工呼吸器の設計について解説する．メイン・システムが機能しなければサブシステムに切り替え，ポンプが動作しなければ電磁弁で代替するなど，非常時にも機能を果たすことのできるシステムを開発した．システムの機能とユーザの安全をどのように確保するのかという考え方は，医療機器以外の分野にも応用できるだろう．

（編集部）

人工呼吸器は生命維持装置の一つです．水難事故などで呼吸が止まった人を助けるのに，口から息を吹き込む方法がありますが，人工呼吸器はそれを病室などで行う装置です．肺機能が低下した患者のほか，全身麻酔からの覚醒過程でも用いられます．

人工呼吸器の基本原理は空気ポンプです．最も簡単な方法では，ふいごやバッグを手で操作して空気を送り込みます．この際，熟練した医師なら自然に行っていることですが，送り込む空気の流量や周期は患者の体格に適したものでなければなりませんし，少しでも自発呼吸がある場合は，それを補助するように呼吸と同じタイミングで空気を送り込まなければなりません（補助呼吸）．

このようなことから，人工呼吸器は圧力（気道圧）や流量（換気量）などのセンサを備え，それらの情報をもとにポンプの動作を制御するのが一般的です（**図1**）．

センサにて自発呼吸を検出（吸気トリガ）したらポンプを起動，あるいは弁を開放して，患者にとって十分な1回分の換気量が得られるように空気を送ります．トリガ待ちがタイムアウトすれば自発呼吸が弱くなったと判断し，必要な時間当たりの換気量が得られるように空気を送ります（強

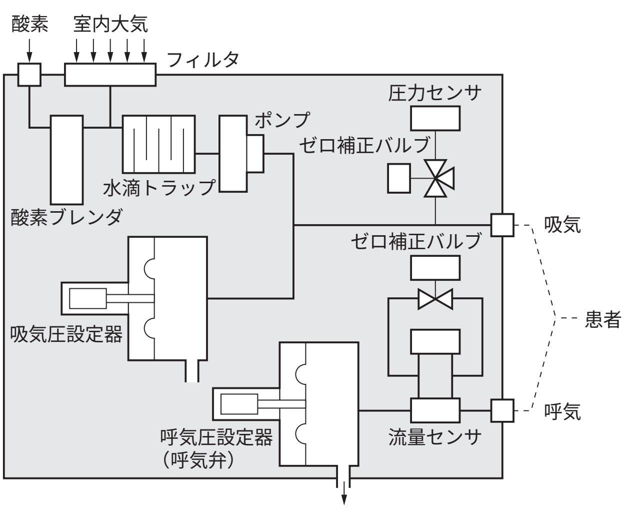


図1　人工呼吸器の構造例

人工呼吸器の構成の概略を示す．患者の自発呼吸を検知しながら，呼吸に合わせて，酸素と室内大気を混合した空気を送る．

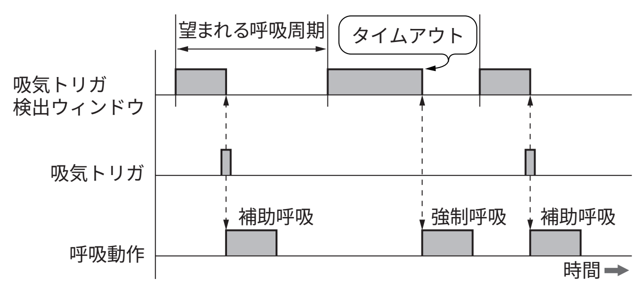


図2　補助呼吸と強制呼吸の動作タイミング

一定時間内に吸気トリガが発生しないとき，強制呼吸を起動させる．

KeyWord　セーフティ・クリティカル，医療機器，信頼性，安全性，アラーム，TCB

制呼吸）．

補助呼吸と強制呼吸の動作タイミングを**図2**に示します．

● 呼吸だけは止めてはならない！

人工呼吸器と患者を制御系として考えると，人工呼吸器の制御はパラメータの多様さ，患者の様態変化という外乱要素が多いことなどで，第1級の複雑さを持っていると言えるでしょう．コンピュータの進歩とともに，装備も年々複雑になってきています．

しかし，絶対におろそかにしてはいけないことがあります．それはシステムが停止しないこと，暴走しないことです．生命を預かる以上当然のことですが，高機能と両立させるには，しっかりとしたコンセプトを持ってシステムの構築にかからねばなりません．

以下，1980年代初頭から1990年代前半にかけて開発され，病院や在宅医療の現場で使われた複数機種の人工呼吸器について解説します．ただし「人工呼吸器はすべてこの通りになっていて，このように設計すべきである」と主張しているのではありません．本稿における信頼性や安全性に関する考え方が参考となれば幸いです．

● 機能は縮小しても動作するバックアップを設ける

人間が作ったものはいつか故障して止まります．人工呼吸器は代替器のつなぎ替えを待っている余裕がないので，可能な限り2重化が望まれます．しかし，それを徹底しようとすると，コストや体積の面で商品価値がなくなってしまいます．そこで，メイン・システムが故障してもその動作の基本的な部分を受け継いで動作するサブシステムをバックアップとして用意しました．

図3にその構成を示します．換気量などを算出する基（デフォルト・パラメータ）となる体重は，ロータリ・スイッチで設定します．ロータリ・スイッチはメイン・システムとサブシステムの両方に接続されているので，動作の引き継ぎに役立ちます．

メイン・システムは，患者の体重を基に，1回当たりの換気量と呼吸回数の推奨値を求め，これをデフォルト値としてまず動作します．その後，必要に応じて各種の動作パラメータをキーボードを用いて設定します．

もし，メイン・システムに異常が起こった場合，サブシステムはメイン・システムの動作パラメータのデフォルト値を引き継いで動作します．体重設定の入力にロータリ・

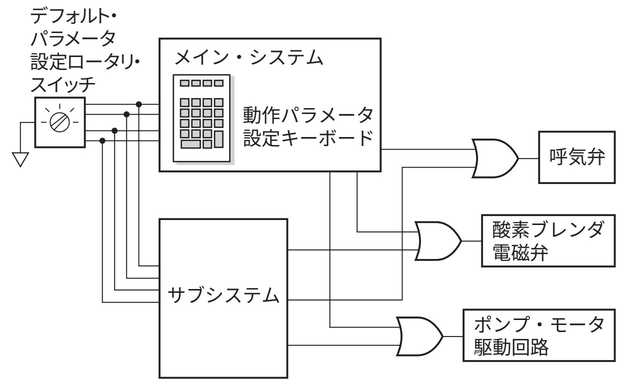


図3　機能が落ちてもサブシステムで動かせるようにした例
機構はメイン・システムとサブシステムのどちらによっても動作する．

スイッチを使用したいのは，使い勝手の問題もありますが，メイン・システムの動作がどうあろうとも同じ値が読み取れるからです．もし，テンキーなどで設定するようにすると，メイン・システムがおかしくなったときはキー・スキャンも止まるため，設定した値は消えてしまいます．ロータリ・スイッチに標準ロジックICの入力側がつながっているだけなら，サブシステムからの読み込みに影響を与えません．

サブシステムは信頼性を第一に，少ない部品点数で構成しました．吸気のセンサは接続されておらず，補助呼吸の機能は持っていません．メイン・システムがダウンしたときに，決まった周期で強制的に空気を送り込む動作だけを行います．そのため，もし切り替えが発生すると，自発呼吸がある患者にとっては急に苦しくなってしまいます（呼気のタイミングが合わないとせき込む）．

あるとき，某所で人工呼吸器がサブシステムの動作に切り替わったという報告を受けました．このとき，全体が止まらなくてよかったと思うと同時に，患者のことを思うと自分も息苦しくなったような気がしたものです．

● バックアップのバックアップを用意

ほとんどの場合，このサブシステムへの切り替えで最悪の事態にならないはずですが，サブシステムが制御するポンプ（この製品ではふいごをモータにより伸縮させるポンプを内蔵）が故障したらどうするかという問題が残りました．そこで採ったのが，酸素のブレンダ（混合装置）に使っている電磁弁を開閉させることにより，強制呼吸もどきを作る方法でした．圧力は制御しないものの，必要な酸素は患者に供給されます．酸素が配管されている病室でなけれ

6

ばこの動作はできませんが，特に部品点数を増やすことなしに「最終バックアップ動作」を実現できました．

このように，「呼吸を止めてはならぬ」というコンセプトを基に，2重3重のバックアップを用意しました．機能の完全な2重化でなくても，最も必要な動作は何かを見極めれば，結果として高い信頼度を持たせることができます．仮に製品コストに目をつぶったとして，システムを完全に2重化しても，保守まで考慮すると信頼度は決して倍まではいかないものです．総合的な見地に立って全体の構成を考えなければなりません．

● アラームは別系統に

止まってはならない人工呼吸器ですが，たとえ止まったとしてもアラームが鳴り，3分以内に駆けつけて相応の処置を施せば，生命にかかわる確率は低くなります．そのため，アラームの発生回路は非常に重要です．アラームが鳴っても駆けつけなければ看護師の責任，アラームが鳴らなかったらメーカの責任となります．

鉄則は，コンピュータが動作していなくてもアラームが出るようにしておくことです．アラーム回路を単独でも動作するように組んでおけば，システムがどのようにおかしくなってもアラームだけは出ます．アラーム回路は信頼性を上げるため，部品点数を少なくすることが望まれます．

人工呼吸器で一番大切な動作は呼吸を途切らせないことですから，最重要のアラームは無呼吸アラームです．どんなことがあっても，これだけは動作しなければなりません．

人工呼吸器は自発呼吸の検出（吸気トリガ）を待って動作するモードもありますが，20秒も待つようだったら（患者の様態変化が疑われる），必ず強制呼吸を行うようにプログラムが組んであります．つまり，20秒を過ぎてもシステム（強制呼吸）が動作しなかったら，プログラムが正常に動いていないことになります．

このような状況をコンピュータとは独立に監視するには，リトリガラブル・ワンショット・パルス・ジェネレータ相当の回路を用意し，20秒間吸気トリガ信号が来なかったら出力がアクティブになるようにしておきます．

図4に，（強制呼吸に伴う）圧力の上昇が約25秒ないとブザーが間欠的に鳴るようにした回路を示します．圧力センサとしては，圧力が上がるとふくらむバルーンに突起物を付けておき，その突起物をフォト・インタラプタで検出する仕組みを用意しました．これなら無調整で長寿命です．複数の機種に用いて良好に動作しましたが，今，あえて見直すとすれば，*CR*の発振回路に高インピーダンスの部分があるため，結露などで基板の絶縁が低下したときに動作しなくなる不安があります．同等の機能を小型マイコンで実行すれば部品点数もさらに減り，より好ましいと思います．

アラーム回路の設計において，後から気づいた重大な点がありました．それは，何が起こったのかを明確に表示しなければならないことです．具体的には，現場から報告があったとき電話1本で状況が把握でき，的確に指示できるようにしなければなりません．例えば，LEDランプやブザーを間欠的に動作させ，その周期でアラームの種類を区別するような方法を採ったとしましょう，しかし，一刻を争うような現場では，このような開発者にしか分からないような識別法は全く役に立ちません．電話ではせいぜい「ピーピー鳴ってます」くらいの情報しか来ないので，何のアラームかさっぱり分かりません．（簡素さと堅牢さは両立しにくいのだが）何が起きているか分からないアラームは，出しても無意味です．どんな機器でもそうですが，使う人の身になって設計しなければなりません．

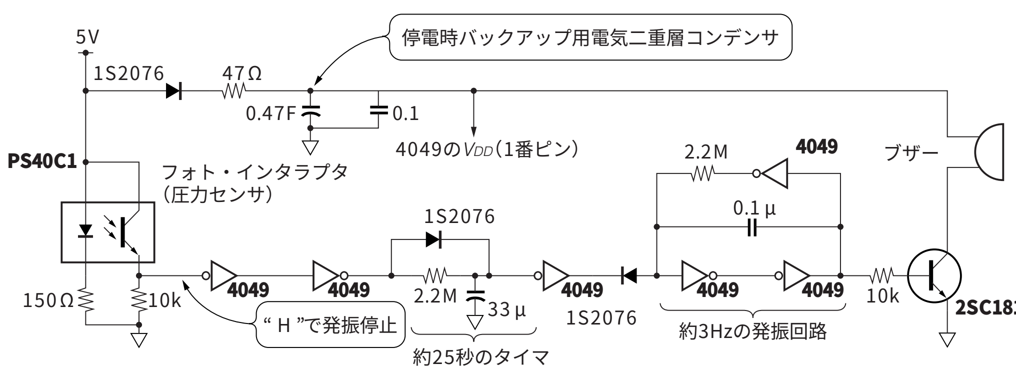


図4
停電検出を兼ねたアラーム発生回路
圧力の上昇が約25秒ないと，ブザーが間欠的に鳴る．

● **異常時に有効な自己診断**

図4に示したアラームは，システム全体を25秒周期のウォッチドッグ・タイマで監視するのと同じ機能を果たします．もちろん，CPU基板にもウォッチドッグ・タイマを設け，異常動作に対してリセットが掛かるようにしています．しかし，CPUの動作そのものがおかしくなっているときに，「自身が異常と判断したら自らリセットする」というアルゴリズム自体，矛盾を含んでいます．真に有効な監視方法は何か？ と考えると，大変なことになってしまいます．以下に解説するのは「自身の異常を知る方法」として試みた例です．

人工呼吸器のプログラムはマルチタスク構成で，呼吸をつかさどるタスクが常時実行状態にあり，その上位レベルにアラームや動作パラメータ変更のためのユーザ・インターフェースのプログラムが随時実行されるという構成になっています．

プログラムが正常に実行されなければ，タスクの切り替えも正常に行われないでしょう．それなら，タスクをコントロールするメモリ領域におかしな値が書き込まれるかもしれないと考えられます．それを検出すれば，異常動作を見つけることができそうです．もし見つかったなら，すべてのタスクを再起動して，正常動作に戻せばよいでしょう．そのような考え方でシステムの骨組みを作りました．**図5**にその動きを示します．10秒ごとに，TCB（task control block）のチェック・サムを計算するタスクが，ほかよりも高い優先順位で実行されます．

この手法は，電源の一時低下や基板に導電性のゴミが落ちたようなときに効果を発揮したかもしれません．しかし，シミュレーションの仕方や効果の検証法に問題があり，実際の製品に搭載するには至りませんでした．機会があればまた別の分野で役立てたいと思っています．

● **本質的な動作を把握する**

人工呼吸器をマイコンで制御し始めた1980年代の初頭

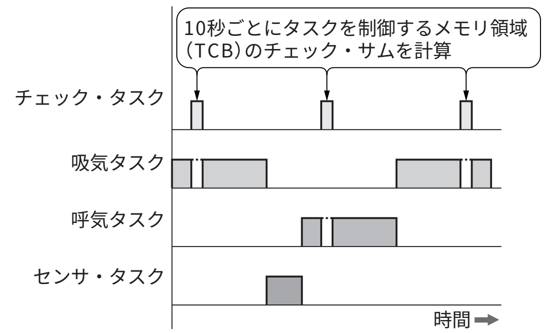


図5　信頼性向上を狙ったマルチタスクの動き
各タスクが実行されると，タスクを制御するメモリ領域（TCB ; task control block）に情報が書き込まれる．TCBのチェック・サムを計算するタスクを用意し，より高い優先順位で動作させる．チェック・タスクは定期的にTCBの正当性をチェックし，異常があればシステムを再起動する．

は，今と比べれば同じ機能を実現するにも大変な数の部品が必要でした．しかも，信頼性も未知数とあって，最初の製品開発にはとても神経を使ったものでした．本稿で述べた手法はその過程で生まれたものです．集積度が上がった今日でも，考え方は依然生きていると思います．

人間業（わざ）ですから，完ぺきなシステムは作れません．しかし，何が本質的な動作かをつかんで設計していれば，事故が起こったときの影響をより少なくすることができます．もし，設計上の問題を指摘されることがあっても，確たる設計思想を持っていれば納得のいく説明ができますし，良い対策を考えてくれる人も現れることでしょう．製品が完成したときの達成感は，このような日々の思索と失敗の積み重ねの上に得られるのです．

やながわ・せいすけ

<筆者プロフィール>
柳川誠介．マイコン草創期，ベンチャーを旗印にしながらリレー・シーケンスしか知らない上司のいる会社を辞め，医療機器製造会社に就職，人工呼吸器に20年ほどかかわった（正社員でいたのは5年ほど）．その間，画像処理システムなどを手がけた．現在は，双方向通信ができる鍵を持つ錠前装置の製品化を進めている．

Design Wave Advance　好評発売中
四則演算，初等超越関数，浮動小数点演算の作りかた
ディジタル数値演算回路の実用設計
鈴木 昌治 著
B5変型判 256ページ　定価3,570円（税込）　ISBN4-7898-3617-7
CQ出版社　〒170-8461　東京都豊島区巣鴨1-14-2　販売部　☎（03）5395-2141　振替 00100-7-10665